CLAIMS

WE CLAIM:

1. A safety controller comprising:

a processing unit having a processor executing instructions, and a memory holding instructions and data, the processing unit providing a hardware lock preventing writing of at least a portion of the memory as controllable by a lock instruction wherein the memory is adapted to hold a standard program and safety program, the safety program requires higher reliability execution than the standard program; and

a lock management program executable on the processing unit unlocks a portion of memory holding the safety program at times when the safety program is executing and locking the portion of memory at other times.

2. The safety controller of claim 1 wherein the portion of memory also holds data operated on by the safety program.

3. The safety controller of claim 2 further including I/O circuitry exchanging input/output values with an external machine and wherein the data includes input/output values.

4. The safety controller of claim 1 wherein the lock management program executable on the processing unit is different from the safety program.

5. The safety controller of claim 4 wherein the lock management program executable on the processing unit is an operating system running on the processing unit and scheduling the execution of the safety program and standard program.

6. The safety controller of claim 1 wherein the lock management program executable on the processing unit confirms the memory portion is locked at the start of the safety program before unlocking the memory portion and invokes an error if the memory portion is not locked at the start of the safety program before unlocking the memory portion.

7. The safety controller of claim 1 wherein lock instruction is a setting of a register indicating the status of different memory portions as locked and unlocked.

8. The safety controller of claim 1 wherein the hardware lock operates so that the locked portion of memory may be read.

9. The safety controller of claim 1 wherein the hardware lock operates so that different portions of memory may be simultaneously locked and unlocked.

10. The safety controller of claim 1 wherein the lock management program executes to keep the portion of memory holding the standard program unlocked.

11. The safety controller of claim 1 wherein the lock management program is a portion of the safety program unlocking the memory portion at the start of safety program and locking the memory portion at the conclusion of the safety program.

12. The safety controller of claim 1 wherein the portion of memory holding the safety program also holds a copy of selected data generated by the standard program.

13. The safety controller of claim 1 further including a lock check program periodically checking the status of the portion of memory holding the safety program when a safety program is not executing and invoking an error is the memory portion holding the safety program is unlocked.

14. The safety controller of claim 1 further including:

a second processing unit having a processor executing instructions, and a memory adapted to hold a copy of the safety program; and

a synchronization program executable by the processing units to execute the safety program on both processing units and compare execution of the safety programs and to enter a safety state when this execution differs.

15. The safety controller of claim 14 wherein the second processing unit provides a hardware lock preventing writing of at least a portion of the memory adapted to hold a copy of the safety program as controllable by a lock instruction.

16. A method of operating a safety controller having a processing unit with a processor executing instructions, and a memory holding instructions and data, the processing unit providing a hardware lock preventing writing of at least a portion of the memory as controllable by a lock instruction, the method comprising the steps of:

(a) loading a first portion of memory with a standard program and a second portion of memory with a safety program, the safety program requiring higher reliability execution than the standard program;

(b) executing the safety program and standard program at different times and unlocking the second portion of memory at times when the safety program is executing and locking the second portion of memory at other times.

17. The method of claim 16 wherein the second portion of memory also holds data operated on by the safety program.

18. The method of claim 17 further wherein the safety controller includes I/O circuitry exchanging input/output values with an external machine and wherein the data includes input/output values.

19. The method of claim 16 further including the step of confirming the second portion of memory is locked at the start of the safety program before unlocking the second portion of memory and invoking an error if the second portion of the memory portion is not locked before the unlocking.

20. The method of claim 16 wherein lock instruction is a setting of a register indicating the status of different memory portions as locked and unlocked.

21. The method of claim 16 wherein locked memory may be read but not written to.

22. The method of claim 16 wherein different portions of memory are simultaneously locked and unlocked.

23. The method of claim 16 wherein the first portion of memory remains unlocked.

24. The method of claim 16 further including the step of periodically checking the status of the second portion of memory when a safety control program is not executing and invoking an error if the memory portion is unlocked.

25. The method of claim 16 further wherein the safety controller includes a second processing unit having a processor executing instructions, and a memory adapted to hold a copy of the safety program, and including the step of:

executing the safety program on both processing units and comparing execution of the safety programs to enter a safety state when this execution differs.

26. A method of operating a safety controller system comprising the steps of:

(a) accepting program instructions from a user describing the logical combination of input sensor data to produce output control data;

(b) collecting the program instructions into logical tasks;

(c) identifying the task as to one of two levels of reliability, a first level being of higher reliability than the second level;

(d) loading a task of the first level into a first portion of memory and a task of the second level into a second portion of memory;

(d) executing the loaded tasks at different times and unlocking the first portion of memory at times when the task of the first level is executing and locking the second portion of memory at other times.